EXHIBIT D

Duncan A. Buell
850 Hampton Creek Way
Columbia SC 29209
buell@acm.org
803-479-7128

May 17, 2017

The Honorable Brian Kemp
Georgia Secretary of State
214 State Capitol
Atlanta, Georgia 30334
(Via email tfleming@sos.ga.gov)

Re: Supplemental information to May 10, 2017, Request for reexamination of voting system

Dear Secretary Kemp:

I am the technical adviser to the group of sixteen Georgia citizens who have formally requested a review of the voting system under the provisions of Georgia Code §21-2-379.2. We have not received a response to our attached May 10, 2017, letter seeking your immediate reexamination of the touchscreen (DRE) voting system prior to the June 20, 2017, special election in Congressional District 6.

Your office was quoted in the press as stating, "We've received their letter, and we will provide a timeline and cost estimate for the review," and "Georgia's voting equipment is regularly tested by experts and local elections officials across the state. We have complete confidence in its accuracy and security."[1] I wish to reiterate that the review that the citizens request should require no more than one day to review the system documentation and one day to prepare, review, and release your findings. Additionally, the cost of the reexamination should be borne by your office, given its responsibility to provide fair, accurate, and secure elections.

Laboratory testing of machines to federal certification standards is not required to determine whether the machines can be "safely and accurately used" in the upcoming election. Adequate documentation exists in Kennesaw State University's Center for Election Systems to reach the irrefutable conclusion that the DRE system is not secure

[1] http://www.ajc.com/news/state--regional-govt--politics/voters-seek-review-georgia-voting-system-before-6th-district-runoff/FHtMDKqMsW0ojYZppnINKN/

and must not be used for future elections. A review of the records in the public domain demonstrates there is considerable doubt that the voting system is fit for use. Machine testing is not required to reach this conclusion.

We are dismayed that by expressing your "complete confidence in its [the system's] accuracy and security" you have prejudged the system as adequate. Overwhelming technical evidence in the public domain details numerous significant security vulnerabilities in the system and demonstrates that such confidence is misplaced. We are certain that any responsible review of the system documentation and the academic research will rapidly conclude that the system cannot be used with reasonable assurance of its security and accuracy.

We call your attention to three major security issues that have come to our attention and must be considered in your reexamination:

1. Significant security vulnerabilities at the KSU Center for Election Systems

   Exhibit A is a recent internal Kennesaw State University general overview assessment of certain security issues at the KSU Center for Election Systems (CES). The assessment notes several significant security vulnerabilities. It is our view that documented security vulnerabilities create such critical questions of security that the "safe and accurate" use of the voting system cannot be assured for the upcoming June election. Even if all listed CES facility vulnerabilities were currently mitigated, it is quite possible that systems may have already been compromised in one or more ways that will remain undetected. Such potential compromises and security implications to the voting system components cannot be reasonably assessed in the near term.

   The CES security vulnerabilities noted in the assessment, considered in relation to the twelve issues listed in our May 10 letter attached, make it clear that the system cannot be used safely and accurately.

   Indeed, what can be inferred from the KSU report is that security and integrity measures that would be reasonable and obvious in any situation involving sensitive information were not in place at the CES. Such measures were possibly not even thought to be necessary for perhaps extended periods of time prior to the security incident. These measures included an acknowledged poor understanding of risk and a failure to recognize the value of the contents of at least one of the targeted servers, the use of software with well-known vulnerabilities, and a lack of established protocols for handling sensitive information.

We note also that the only "successes" reported are procedural: CES and KSU were able to respond quickly ***when*** disaster struck, although thorough testing of the response effectiveness has apparently not been conducted. There are no successes mentioned that involve preventing disaster or mitigating a disaster's effects, and the lack of such successes only decreases the trust that Georgia's citizens should have in their elections.

2. Significant violations of HAVA Section 301(a)

We call your attention to the legal requirements of the Help America Vote Act that mandate minimum voting system security standards for audit capacity. The Election Assistance Commission (EAC) issued an advisory letter regarding audit capacity compliance on July 20, 2005 (Exhibit B). The system must comply with Sections 2.2.5.2.1 and 2.5.3.1 of the 2002 Voting System Standards.

a. Section 2.2.5.2.1 requires the maintenance of accessible system logs. Fulton County Elections Department has stated that such records cannot be extracted on a timely basis. In fact, they require months of work to retrieve. (Exhibit C—Rocky Mountain Foundation's FOIA response.) The physical security of such audit log information in the memory of the TS machine is inadequate because of lax security of the voting machines themselves in storage between elections as well as at the polling places before and after voting. Additionally, the audit logs can be manipulated and edited by using malware transferred via infected memory cards. Those memory cards can be exposed to malware because of the CES security vulnerabilities noted in paragraph 1 above or through malicious insertion of malware onto voter access cards as a result of lax security of e-pollbooks, such as the April 15, 2017, Cobb County e-pollbook theft.

b. Section 2.5.3.1 lists "Common Standards" required of voting systems. The voting system appears to be in significant violation of certain of those mandatory standards.

(i). Paragraph *f* of this section requires that all audit information be available to be printed. The information includes ballot images (cast vote records) as required in Section 4.5. As noted in Exhibit C and in paragraph a above, such audit data is not, as a practical matter, available from Georgia's voting system.

(ii). Paragraph *g* requires that security must be in place to avoid alteration or destruction of data when election results are transmitted electronically. We question the adequacy of security of transmission of results from TSx units via modem to the GEMS server. Issue 4 of our May 10 letter raised this concern. Additionally, we believe that the encryption key for the TS machine is in the public domain and undermines any security of the votes or results transmitted in any fashion. (See issue 9, May 10 letter.)

3. Significant Violations of FEC 1990 Voting System Standards

It is our understanding that Georgia's system was certified under the Federal Election Commission's 1990 VSS standards, which requires audit trails as "essential for public confidence, for recounts, and in the event of litigation."[2] However, it appears that the system is not in compliance with numerous essential security and accuracy-related provisions of the 1990 VSS. I provide two examples:

a. Similar to the HAVA requirements detailed in paragraph 2 above, VSS Sections 1.3.3, 2.3.2, and 3.2.4.2.5, among others, require the retention and accessibility of ballot images and activity logs. Yet the images and activity logs cannot be retrieved on a practical and timely basis to address transparency, recount, audit, or litigation needs.

b. VSS Section 5.3 requires adequate measures to prevent unauthorized access to the system. As noted in paragraphs 1 and 2a above, the physical security vulnerabilities raised in our letter of May 10, demonstrate that security is critically inadequate and cannot meet the mandatory minimum standards.

Significant noncompliance with *any one of these individual mandatory provisions* for security and accuracy renders the system unsafe for use in the upcoming June election. Considered in combination, the numerous significant violations summarized above and in the May 10 letter provide overwhelming evidence that the system cannot be reasonably certified to be safe and accurate for near-term use.

The clear intent of the provisions of Georgia Code §21-2-379.2 is to provide a failsafe method to assure the security and accuracy of the voting system regardless of the official status of system certification. We wish to make it clear that the mere absence of detected and documented intrusions, malware, or irregularities is not an appropriate standard on

---

[2] page xxiii FEC 1990 Voting Systems Standards

which to evaluate the security and accuracy of the system. The documented areas of current system vulnerability present clear evidence that past and future intrusions could easily go undetected. Given such overwhelming evidence, there is no reasonable path to reach a responsible conclusion that the system is secure and reliable for voter use in the near term.

I reiterate the fact that laboratory testing is not required to ascertain that significant security issues are present. They cannot be overcome in the immediate future. The system documents are sufficient to confirm the existence and proliferation of the serious issues we have noted. A review of these issues can be accomplished and documented in one to two days. We request that you make this issue a priority for your staff and the KSU Center for Election Systems. Your required reexamination of the voting system cannot be reasonably delayed. Early voting in the June 20 special election begins on May 30, and voters must not be permitted to vote on the clearly vulnerable system.

Paper ballots are a safe, efficient, and cost-effective solution for the June 20 election. Given that there is only one contest on the ballot, hand counting of ballots in the precinct is easily accomplished and verified in a short period of time after the closing of the polls. It seems likely that results would be available at least as quickly with hand counting as with electronic tabulations and transmission, and possibly even more promptly.

If your office or the KSU Center of Election Systems has questions about our concerns, I am happy to discuss them at your convenience. Additionally, I have the good fortune of having several computer scientist colleagues who have conducted extensive Diebold voting systems research and who are available to assist with any specific technical issues.

I look forward to hearing from you very soon. Thank you for your consideration in this matter.

Duncan A. Buell

(For informational purposes)
Professor and NCR Chair in Computer Science and Engineering
University of South Carolina
Columbia SC 29209
buell@acm.org
803-479-7128

cc: DeKalb County Elections, H. Maxine Daniels, Director voterreg@dekalbcountyga.gov

Fulton County Elections, Director Richard Barron Richard.Barron@fultoncountyga.gov
Cobb County Election Director Janine Eveler, info@cobbelections.org
David Worley, State Election Board Member, david@ewlawllc.com
Rebecca Sullivan, State Election Board Member, Rebecca.Sullivan@DOAS.Ga.Gov
Judge Ralph Simpson, State Election Board Member, rfs@simpsonmediation.com
Mustaque Ahamad, Atlanta, GA 30306
David Bader, Atlanta, GA 30306
Ricardo Davis, Woodstock, Georgia 30188
Richard DeMillo, Atlanta GA 30305
Virginia Forney, Atlanta, GA 30309
Merrick Furst, Atlanta 30306
Adam Ghetti, Atlanta, GA 30324
Jeff Levy, Atlanta, GA 30306
Rhonda J. Martin, Atlanta, GA 30305
Paul Nally, Rydal, GA 30171
Michael S Optiz, Marietta, GA
Susan McWethy, Decatur, GA
Renee Vorbach, Norcross, GA
Anita Darden, Atlanta, GA
Linda McPherson, Peachtree Corners, GA
Michael Burke, Norcross, GA